BLACK CELL
Protecting critical infrastructures

Kiberbiztonsági támadási technikák szektorspecifikus hőtérképe

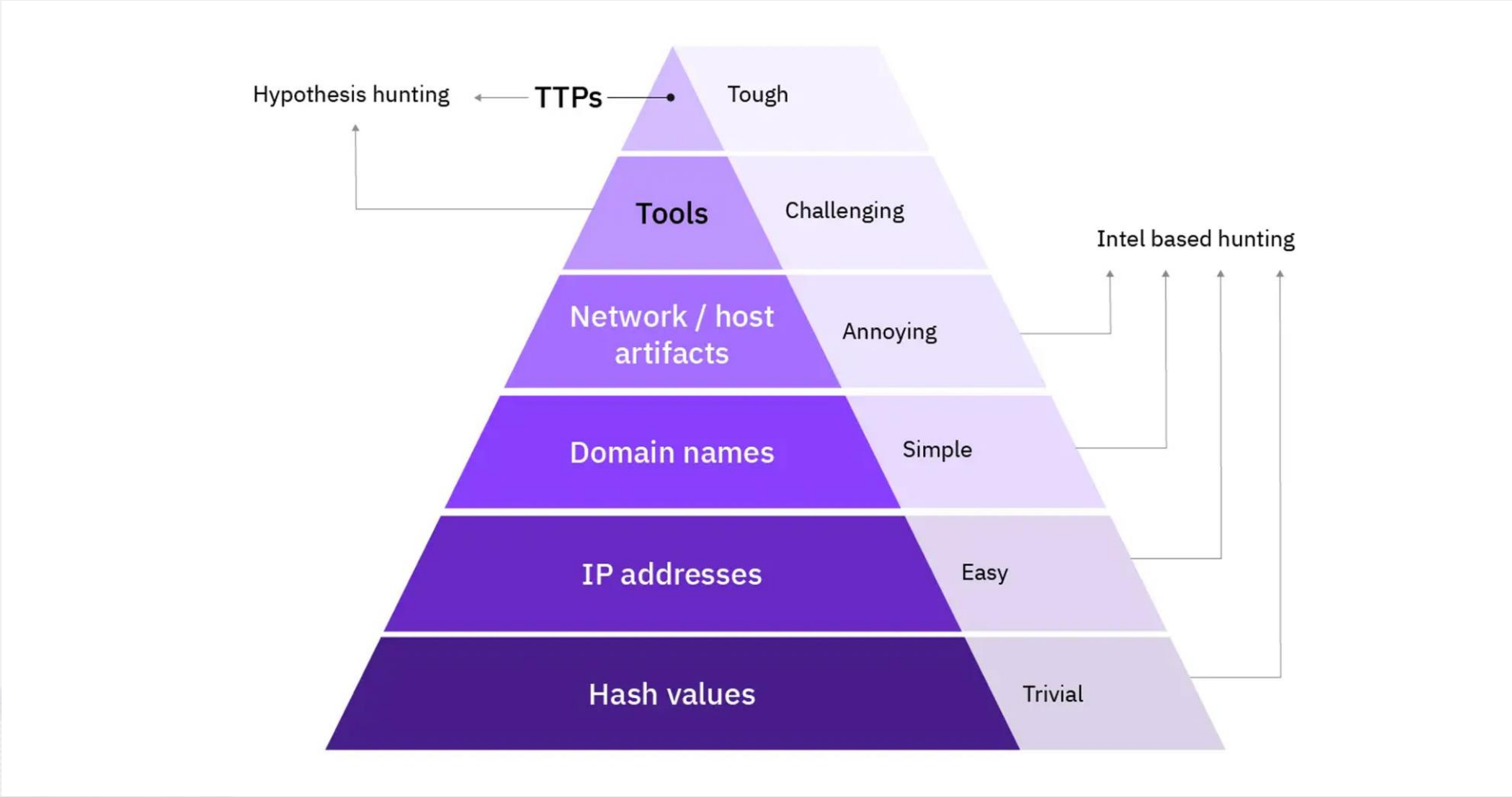
Gyebnár Gergő | Black Cell

TLP:CLEAR

Napirend

- MITRE ATT&CK keretrendszer bemutatása
- Pénzügyi szektort érintő támadások
- Pontozási rendszer
- Heatmap
- Riasztás kialakítása
- Tesztelés
- Kérdések és válaszok

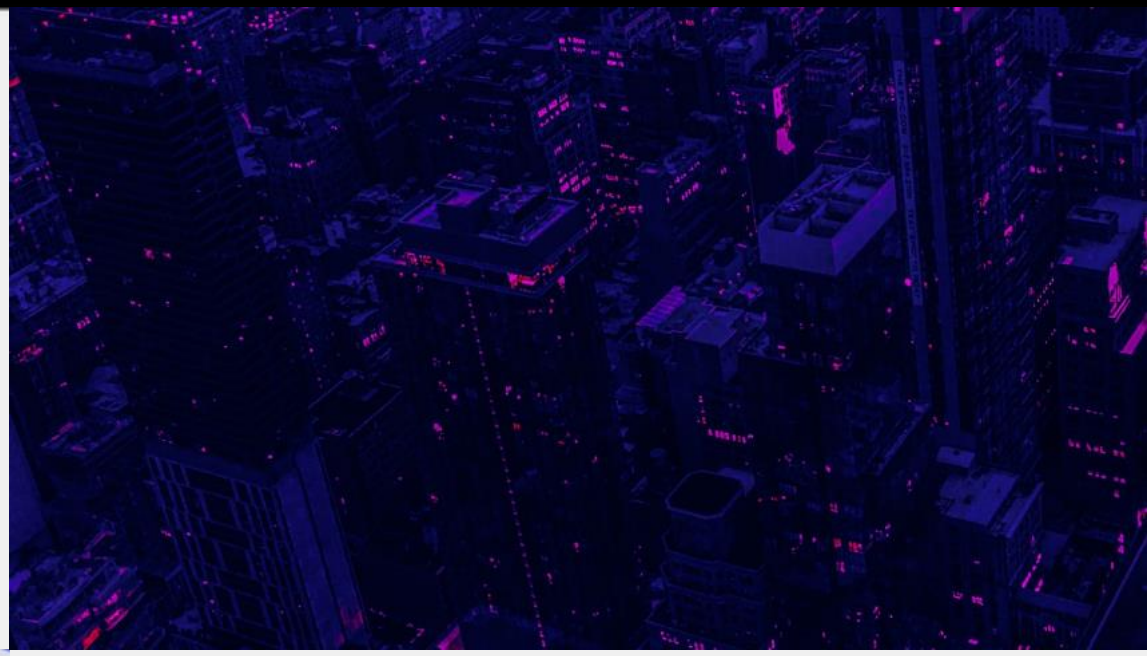
CTI – Cyber Threat Intelligence



MITRE ATT&CK keretrendszer bemutatása

- TTP alapú threat intel
- 3 fő domain: Enterprise, ICS, Mobile
- Enterprise a legérettebb: 14 taktika; 192 technika; 401 al-technika (v12)
- Tökéletes a kiberbiztonság detekciós képességek technikai érettségének nyomonkövetésére
- Nem megfelelően használva hamis biztonságérzetet eredményez
- Egyre több megoldás és keretrendszer támogatja (Sigma; MISP; STIX; stb.)
- MITRE Atlas;)

Pénzügyi szektort érintő támadások



Retrospektív OSINT

Kampányok, incidensek és elkövetői csoportok

Mely technikákra láthatunk példát?

- Silence
- Tonto Team
- WIRTE
- admin@338
- Andariel
- APT-C-36
- APT38
- QakBot
- Zeus Panda
- Dtrack
- BlackTech
- Carbanak
- Javali
- PingPull
- Pysa
- RATANKBA
- Regin
- Rising Sun
- Volgmer
- FALLCHILL
- Hermeticwiper
- TrickBot
- Ember Bear
- GALLIUM
- OilRig
- Silence
- Tonto Team
- Cobalt Group
- Lazarus Group
- FIN4
- Clop
- Cuba
- DarkVishnya
- Deep Panda
- APT19
- menuPass
- Moses Staff
- PoisonIvy
- AppleJeus
- Bankshot
- BOOTRASH
- Dridex

Pontozás

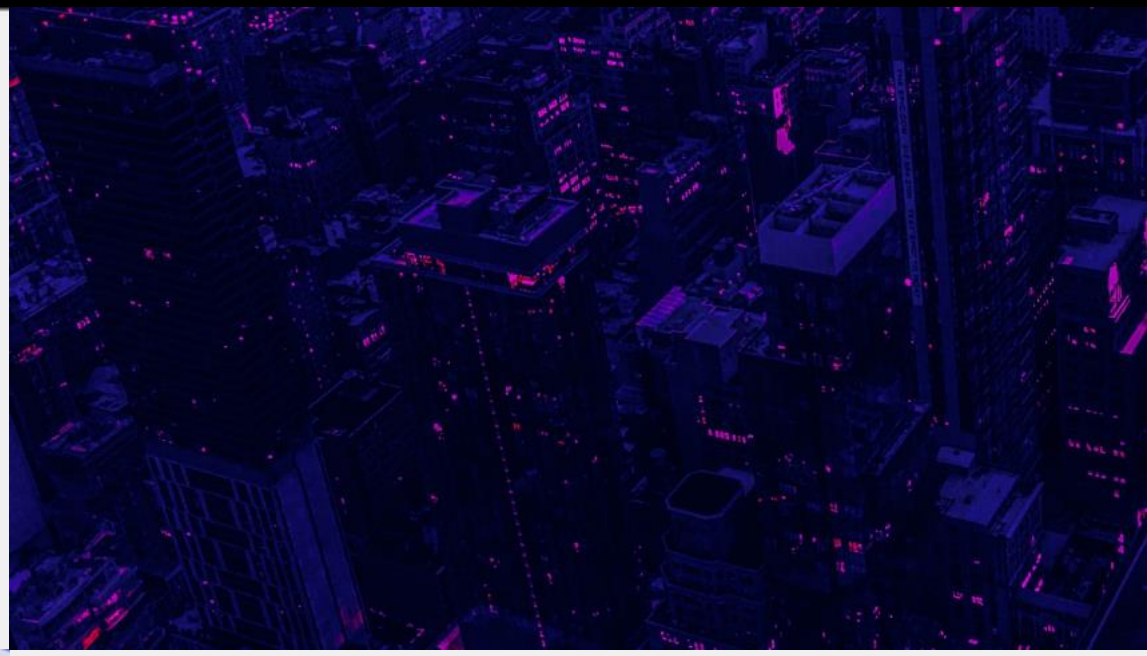
Súlyozás

Layers/score	Impact	Evasion	Complexity	Successfulness	Accuracy	Sum
Cobalt Group	3	3	3	3	1.4	16.8
Lazarus Group	4	4	4	4	1.2	19.2
FIN4	3	3	2	3	1	11
QakBot	3	4	5	3	1.2	18
Zeus Panda	2	3	3	3	1.2	13.2
TrickBot	4	3	4	4	1.2	18
Ember Bear	3	4	3	4	1.5	21
GALLIUM	4	3	3	4	1	14
OilRig	4	3	4	4	1	15
Silence	3	3	4	3	1	10
Tonto Team	4	4	4	4	1.5	24
WIRTE	3	3	4	3	1	13
admin@338	4	2	2	2	1	10
Andariel	2	3	3	3	1.5	17
APT-C-36	3	2	3	4	1	12
APT38	5	3	5	5	1	18
BlackTech	4	3	3	4	1.4	19.6
Carbanak	4	3	3	4	1.2	16.8
Javali	3	3	3	3	0.8	9.6
PingPull	2	2	2	2	1	7
Pysa	4	4	3	4	1	15

Layers/score	Impact	Evasion	Complexity	Successfulness	Accuracy	Sum
DarkVishnya	3	3	3	3	1.2	14.4
Deep Panda	4	3	3	3.5	1.4	18.9
APT19	4	4	4	4	1.5	24
menuPass	4	4	5	4	1.2	20.4
Moses Staff	3	3	3	4	1	16
PoisonIvy	2	2	2	2	1	8
AppleJeus	3	4	4	3	1	14
Bankshot	2	2	5	2	1	11
BOOTRASH	2	5	3	4	1	14
Clop	4	3	3	3	1	13
Cuba	4	3	3	3	1	13
Dridex	4	3	4	5	1	16
Dtrack	4	5	5	4	1	18
FALLCHILL	3	2	3	4	1	12
Hermeticwiper	4	4	3	4	1	15
RATANKBA	3	4	4	3	1	14
Regin	3	3	3	3	1	12
Rising Sun	2	2	3	2	1	9
Volgmer	3	2	2	3	1	10

Heatmap bemutatása

DEMO



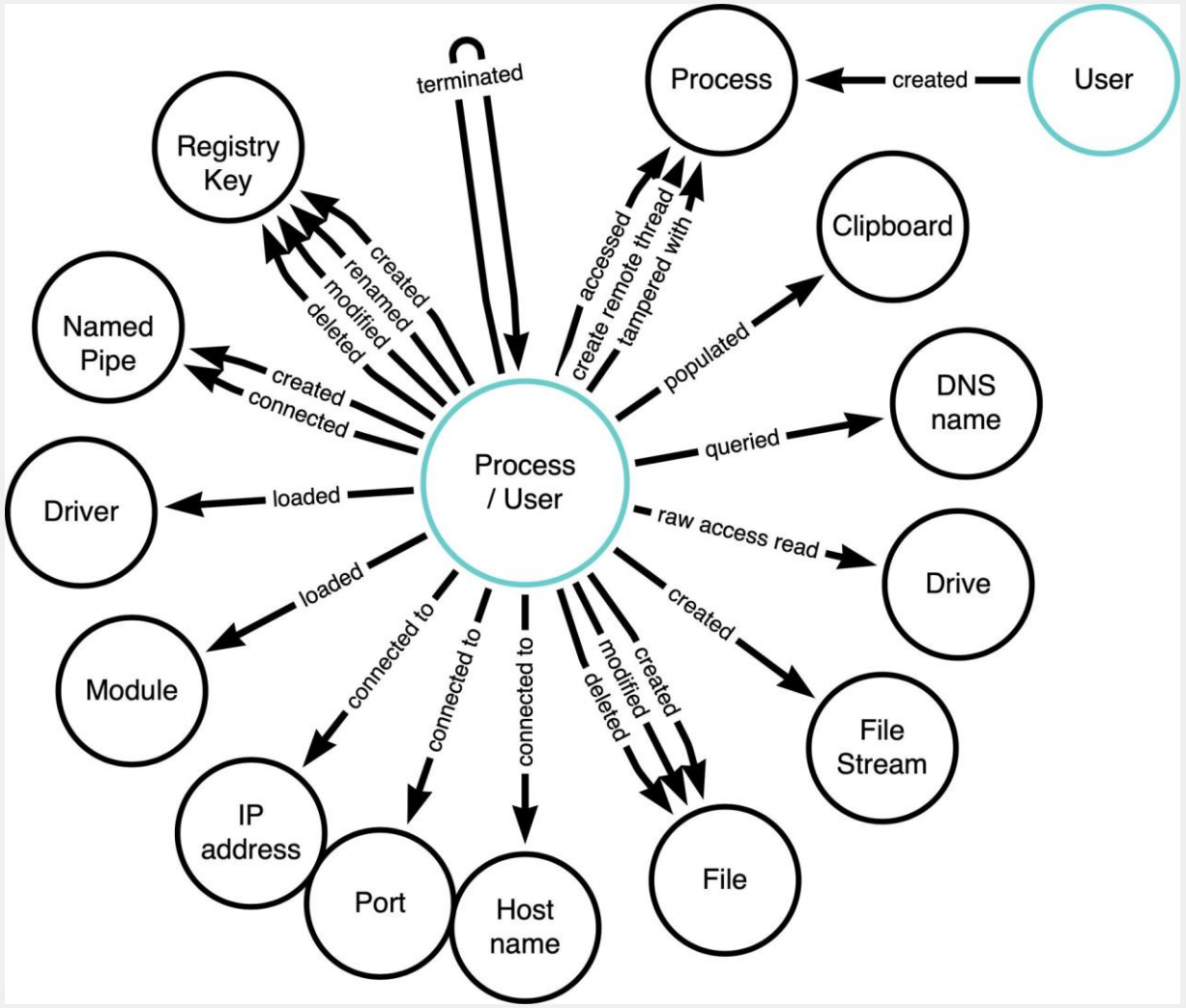
https://mitre-attack.github.io/attack-navigator/

Riasztás kialakítása

Scheduled Task

- Masquerading (T1036) (Trickbot például)
- Process Injection (T1055)
- Disabling Security Tools (T1089)
- Domain Trust Discovery (T1482)
- Remote File Copy (T1105)
- Windows Admin Shares (T1077)

Sysmon



Sysmon

- <!-- Event ID 3 == Network Connection - Includes -->
- <RuleGroup groupRelation="or">
- <NetworkConnect onmatch="include">
- <Image name="technique_id=T1070,technique_name=Indicator Removal on Host" condition="image">wevtutil.exe</Image>
- <Image name="technique_id=T1053,technique_name=Scheduled Task/Job" condition="image">taskeng.exe</Image>

BLACK CELL

Auditd

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command And Control
9 items	10 items	13 items	7 items	22 items	9 items	13 items	6 items	10 items	9 items	21 items
Drive-by Compromise	Command-Line Interface	.bash_profile and .bashrc	Exploitation for Privilege Escalation	Binary Padding	Bash History	Account Discovery	Application Deployment Software	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	Exploitation for Client Execution	Bootkit	Process Injection	Clear Command History	Brute Force	Browser Bookmark Discovery	Exploitation of Remote Services	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Graphical User Interface	Browser Extensions	Setuid and Setgid	Disabling Security Tools	Credential Dumping	File and Directory Discovery	Remote File Copy	Clipboard Data	Data Encrypted	Connection Proxy
Spearphishing Attachment	Local Job Scheduling	Create Account	Sudo	Exploitation for Defense Evasion	Credentials in Files	Network Service Scanning	Remote Services	Data from Information Repositories	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Link	Scripting	Hidden Files and Directories	Sudo Caching	File Deletion	Exploitation for Credential Access	Network Sniffing	SSH Hijacking	Data from Local System	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing via Service	Source	Kernel Modules and Extensions	Valid Accounts	File Permissions Modification	Input Capture	Password Policy Discovery	Third-party Software	Data from Network Shared Drive	Exfiltration Over Command and Control Channel	Data Encoding
Supply Chain Compromise	Space after Filename	Local Job Scheduling	Web Shell	Hidden Files and Directories	Network Sniffing	Permission Groups Discovery		Data from Removable Media	Exfiltration Over Other Network Medium	Data Obfuscation
Trusted Relationship	Third-party Software	Port Knocking		HISTCONTROL	Private Keys	Process Discovery		Data Staged	Exfiltration Over Physical Medium	Domain Fronting
Valid Accounts	Trap	Redundant Access		Indicator Removal from Tools	Two-Factor Authentication Interception	Remote System Discovery		Input Capture	Scheduled Transfer	Fallback Channels
	User Execution	Setuid and Setgid		Indicator Removal on Host		System Information Discovery		Screen Capture		Multi-hop Proxy
		Trap		Install Root Certificate		System Network Configuration Discovery				Multi-Stage Channels
		Valid Accounts		Masquerading		System Network Connections Discovery				Multiband Communication
		Web Shell		Obfuscated Files or Information		System Owner/User Discovery				Multilayer Encryption
				Port Knocking						Port Knocking
				Process Injection						Remote Access Tools
				Redundant Access						Remote File Copy
				Rootkit						Standard Application Layer Protocol
				Scripting						Standard Cryptographic Protocol
				Space after Filename						Standard Non-Application Layer Protocol
				Timestomp						Uncommonly Used Port
				Valid Accounts						

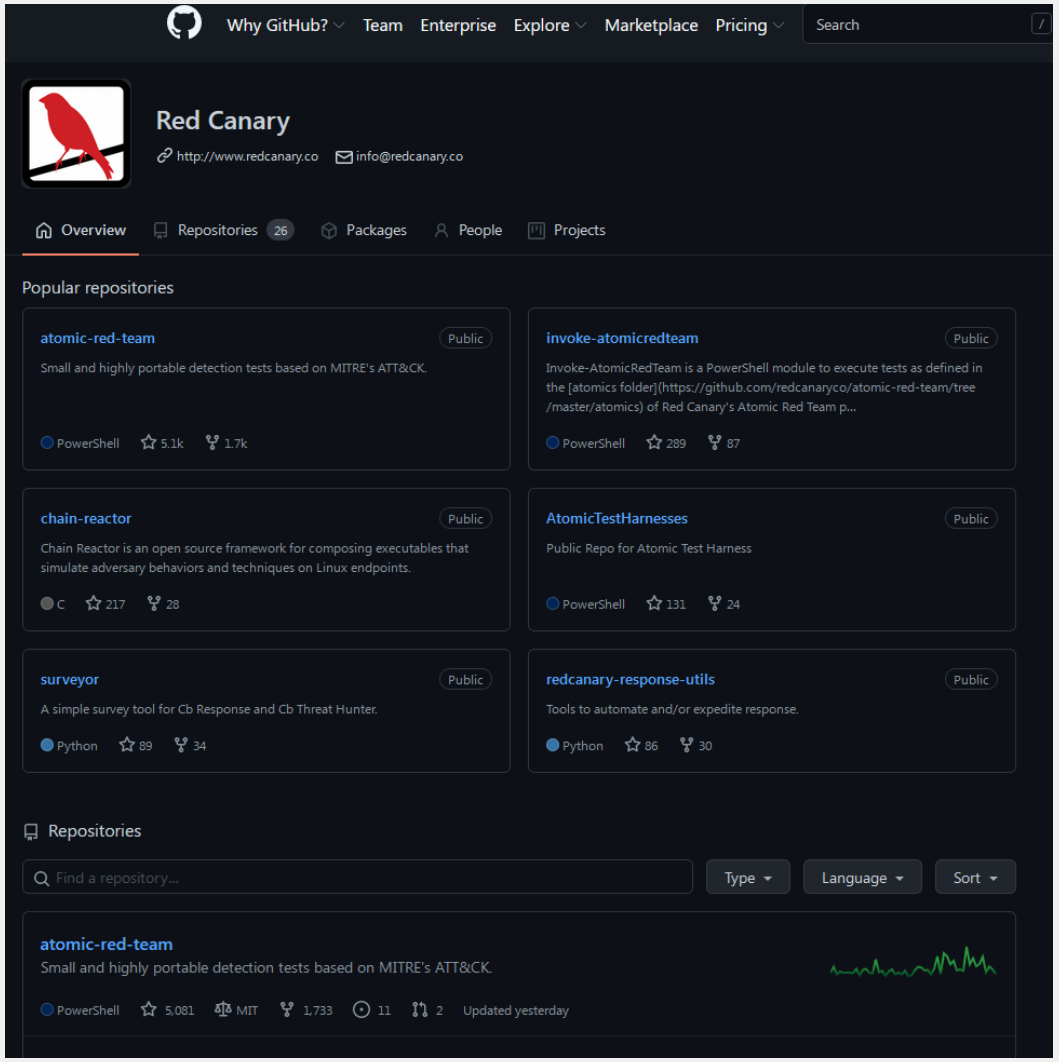
Sigma by Florian Roth

```
title: Scheduled Task Creation
status: experimental
description: Detects the creation of scheduled tasks in user session
author: Florian Roth
logsource:
    category: process_creation
    product: windows
detection:
    selection:
        Image: '*\schtasks.exe'
        CommandLine: '* /create *'
    filter:
        User: NT AUTHORITY\SYSTEM
    condition: selection and not filter
fields:
    - CommandLine
    - ParentCommandLine
tags:
    - attack.execution
    - attack.persistence
    - attack.privilege_escalation
    - attack.t1053
    - attack.s0111
falsepositives:
    - Administrative activity
    - Software installation
level: low
```

https://github.com/SigmaHQ/sigma/tree/master/rules

Tesztelés

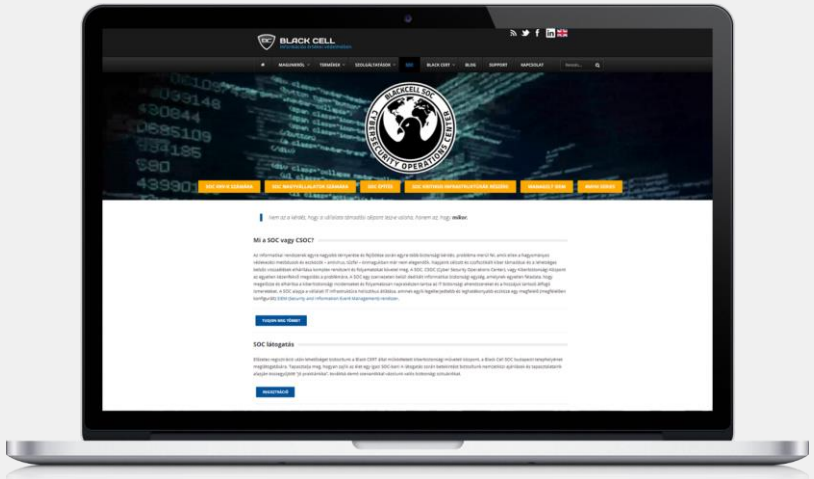
- Atomic Red Team
  - https://atomicredteam.io/atomics/
- Caldera
  - https://caldera.mitre.org/



Naprakészen tartás

Elérhetőségeink

Kérjük, hogy látogasson el weboldalunkra, írjon nekünk egy e-mailt, vagy lépjen kapcsolatba közvetlenül Ügyfélkapcsolati Menedzserünkkel!



https://blackcell.io/

info@blackcell.io